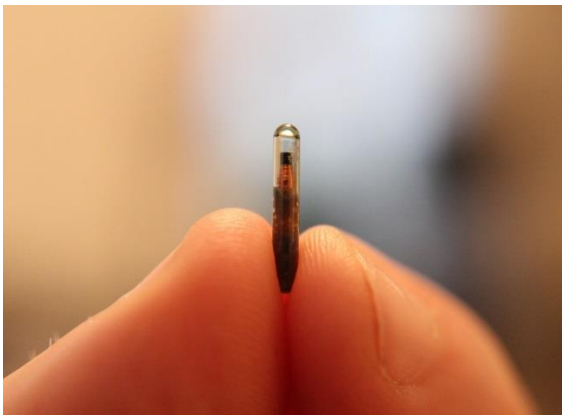

Microchipping humans: a futuristic utopia or a dystopian future?

What started as the development of technology for automatic identification of physical objects has now been shifting towards the identification of humans. The so-called radio-frequency identification (RFID) technology is not new, it is already integrated into bankcards, ID cards, transport cards and even pets, but now people are increasingly considering implementing this technology in themselves for various reasons and uses. But are RFID implants that different from all the cards and badges that we normally carry in our everyday life? Are they really more dangerous?

What is the RFID technology and why do we care?

Recently, a Belgian company offered its employees the possibility of implanting an RFID chip to facilitate access to the company's assets such as buildings and rooms as well as IT systems and laptops. This is not the first company in Europe to make such a proposal that in fact has been warmly welcomed by some employees. The RFID tag or microchip is about the size of a grain of rice, it is usually inserted into the human hand, between the thumb and index finger and it contains data that can be transmitted over short distances to special receivers or readers. This RFID chip is passive, as it only transmits the data to the appropriate reader when it is in proximity to it and, since it is powered by the reader's signal, it does not need a battery.

The emitted signal frequency is quite low, requiring a close distance in order for the reader to be able to receive the data. The RFID chip can also hold small amounts of data and so it usually only contains a unique identification number that can be then linked to information such as a name, address, birthday, gender and even financial or health information, stored in an external computer database. This way, a person with an RFID chip can have doors opening as she passes by or unlock her computer while reaching for it. In addition, a doctor could receive all medical information for a patient and a consumer could pay for her groceries with a single scan. Before getting too excited or too freaked out over this human implanted microchip, some security, privacy and data protection questions should be posed.

So how about legal implications and ambiguities?

First of all, as the reference to the chip's unique identification number can indirectly identify a natural person, this data is considered to be personal under the European personal data protection regime. According to these EU legal instruments, the controller is the one determining the purposes and means of the processing of personal data and is thus responsible for the security of the data as well as the exercise of the data subject's rights. Therefore, when personal data are stored on the chip, the controller will be the party who has opted for the use of the implantable chip as a means of storing personal data and who has decided which type of data will be stored on it. In the context of microchips implanted in employees, it is arguably the company acting as the data controller, as it will be the one

determining the purposes of the processing, which, in this case, refers to the extent of accessibility to company assets that will be provided by the chip. A chip is only implemented when the person has consented to it, and so consent is the legal ground for the processing of the data, which however is restricted only to specific purposes of, for example, acquiring access or making a payment.

So far so good. A human implanted microchip does not necessarily differ essentially from the microchip integrated in a card or a badge; the same personal information can be linked to both chips while both require proximity in order for the data to be transmitted. However, the implanted chip's essential feature can potentially make all the difference. As it is permanently attached to the human body, unless it is surgically removed, and as technology advances radically, the possibilities are endless. RFID chips can now be connected to the cloud and even mobile phones, they can function both as read-only and as read-write, while their storage, processing and communication capacities will only get more sophisticated.

Constant tracking and human hacking may become a reality

In order to track an RFID chip, it is necessary that RFID readers are deployed in public. However, as the capabilities of the chip to connect to more and diverse kinds of readers increase, the possibility for the chip to transmit its data to them and for anyone nearby to identify and track the person in whom the chip is implemented also increase. In this way, every move a human who has implemented an RFID chip in herself makes can be tracked, albeit only by maintaining a close proximity. Distance however may not even be a restriction over time as the technology evolves. Of course, as technology advancements will have the same impact on chips integrated inside the cards humans already carry on themselves, the true risk lies with the fact that one cannot choose to take the chip off and back on. In a perfect, law obedient society, technology will only elevate the quality of life. However, in reality the risks of illegal human tracking may augment along with the implantation of microchips.

Another scenario that could rise from human implantable microchips depending on their rapidly growing capabilities is human bodies becoming a target or a tool for cybercrimes. Currently, cyber-attacks are committed online by the use of electronic communications networks and information systems against computer networks and computer systems. Implantable chips are potentially vulnerable to a variety of already established cyber-attacks. Information stored on the RFID chip can be read but even more so it may be altered or copied, resulting in the replication of one's identity. However, along with the radical improvements in technology, a human implantable microchip may even become vulnerable to computer viruses. Apart from the legal implications of bodily integrity, a new generation of cybercrime, where humans are being infected with computer viruses may emerge.

To sum up

Human implantable microchips bring the practical advantages of not worrying about getting your card stolen or lost and of being able to merge different sorts of everyday information into one small piece of technology that is always ready to use. Identification via such means without doubt is both an advantage in certain cases (e.g. when authorized access is required or in case of a medical emergency), and a drawback in others (e.g. where it provides the opportunity for illegal activities like identity theft or illegal human tracking). As security risks seem to be higher than the improvements in our quality of life and as various ethical questions arise with this practice, one cannot help but wonder whether there is actually added value in human implantable microchips and whether it can outweigh the risks and possible harms.

Category: Privacy and Data Protection, Security and Cybercrime

Keywords: RFID, human, implantable, microchip,